NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

MANDAR MIRASHI, Plaintiff, v. JOHN DOE, Defendant (unknown individual) v. 521.99931468 Bitcoin, *In rem* Defendant v. FIXED FLOAT, KRAKEN, CHANGENOW, EXCH.CX, TRADEOGRE, & JOHN DOE EXCHANGE(S) Relief Defendants	No. 25cv1805 (EP) (LDW) **OPINION**

Plaintiff Mandar Mirashi alleges that an unknown perpetrator (the "Hacker") hacked his email and cryptocurrency wallets and stole approximately $40 million worth of Bitcoin. D.E. 1 ("Complaint" or "Compl."). Plaintiff moved for an *ex parte* temporary restraining order ("TRO") generally freezing his stolen Bitcoin. D.E. 2-1 ("Motion" or "Mot."). The Court granted the TRO and construed the Motion as also seeking a preliminary injunction in accordance with Federal Rule of Civil Procedure 65. D.E. 5. The Court held a hearing on the Motion on March 20, 2025 (the "Hearing"). The Court has reviewed the Motions and all other relevant items on the docket, and has considered the argument and evidence presented at the Hearing. For the following reasons,

the Court will **GRANT** the Motion and enter a preliminary injunction as set forth in the accompanying Order.

I. BACKGROUND

A. Factual Background

As of February 27, 2025, Plaintiff owned 521.99931468 Bitcoin which he kept in two cryptocurrency wallets with blockchain addresses 36cfw3QiQeJJryX7JbWb1DKL7ZP1zMuF1S ("Plaintiff Wallet 1") and 33oV5phadHeUPEgjVNH9fVUZsNhAeDLhAN ("Plaintiff Wallet 2"). D.E. 2-2 ("Pl. Decl.") ¶ 3.

On the afternoon of February 25, 202[5], Plaintiff received an email purporting to be from Google concerning account access by relatives of a deceased person. *Id.* ¶¶ 4-5. Plaintiff clicked on a link titled "Case File," entered his Google login credentials on the page that link opened, and was directed to what appeared to be a Google chat portal where he attempted to inquire into the account access notification. *Id.* ¶¶ 6-7.

Later that evening, Plaintiff received an email from "support+recover@ledger.com," which appeared to be from Ledger, a brand of "cold storage" wallet used to keep cryptocurrency keys secure. *Id.* ¶¶ 9-10. The email referred to a "recovery request" that Plaintiff had submitted, and stated that if Plaintiff had not submitted a recovery request, he needed to take immediate action by clicking on a link in the email, providing his "extended public key" and requesting that the recovery request be cancelled. *Id.* ¶ 12. Plaintiff had not initiated a recovery request and contacted Ledger to inform them that he believed he was the target of a phishing scam. *Id.* ¶¶ 13-14. Plaintiff exchanged emails with Ledger but is unaware which emails were legitimate and which emails were not. *Id.* ¶ 15.

Plaintiff turned to Reddit for guidance and posted on a Reddit page asking if others had seen similar emails from Ledger. *Id.* ¶ 19. After receiving various conflicting reports from the

Reddit community, Plaintiff noticed that his Reddit account had been deleted by an unknown user and he could no longer access the responses to his post. *Id.* ¶¶ 20-22.

The night of February 26, 2025, in light of the suspicious activity, Plaintiff moved 300 BTC out of his Ledger wallet and into another cryptocurrency wallet, Electrum, and went about changing various passwords, including his Google password. *Id.* ¶¶ 24-25. Plaintiff never clicked on the link contained in the February 25 email from support+recover@ledger.com and never provided his "extended public key" or "private key" details to anyone. *Id.* ¶ 26.

However, that same night, Plaintiff saw a pending transaction on the Bitcoin blockchain which attempted to move 302 BTC from Plaintiff's Electrum wallet to an address he was not familiar with: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. *Id.* ¶ 27. Plaintiff immediately took steps to halt this transaction and was successful in preventing it from moving forward. *Id.* ¶ 28. Believing that his Electrum wallet was compromised, Plaintiff moved his Bitcoin back to his Ledger wallet. *Id.* ¶ 29.

The next day, February 27, 2025, Plaintiff discovered that 521.99931468 BTC had been transferred from his two Ledger wallets and sent to the following address: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. *Id.* ¶ 30. Smaller amounts of other cryptocurrency assets were also missing from Plaintiff's Ledger and Metamask wallets, leaving the wallets completely empty. *Id.* ¶ 31. Plaintiff subsequently contacted the police and the FBI. *Id.* ¶ 32.

To assist in tracking and recovering the missing Bitcoin, Plaintiff retained Blockchain Forensic Roman Bieda ("Blockchain Forensic"), a Blockchain analysis company. TRO Mot. at 2. On March 5, 2025, Blockchain Forensic submitted a report on the "theft and subsequent

movements" of Plaintiff's Bitcoin. *Id.* (citing D.E. 2-4 ("BF Report")). Blockchain Forensic concluded the following:

- The Hacker transferred 521.99931468 BTC from Plaintiff's wallets to the Hacker's address: bc1q8fvx5trkyfvt9xmj43pmum9de76lhq0euntngr. BF Report ¶ 12.
- The funds were then "distributed through a complex layering system designed to conceal the source of the money." *Id.* From the Hacker's address the Bitcoin was split up and spread out in 668 transactions to 197 different "singe-use" private (unhosted) addresses and to 140 addresses associated with blockchain services. *Id.* ¶¶ 12-14.
- Approximately 354.4 of Plaintiff's Bitcoin was deposited in accounts held by the following cryptocurrency companies: FixedFloat, Kraken, ChangeNow, exch.cx, TradeOgre, and unknown (John Doe) Exchange(s) (together, the "Relief Defendants"). *Id.* ¶ 14.
- Another approximately 139.41 BTC remain in wallets controlled by the Hacker:
    - bc1qedyy7dfqz7kcesk8ap5kv0sq90c0cctv75fjda;
    - bc1q5uhs4kwaq685hx2p9klhzufw6kzck65x9znvua;
    - bc1qwjtuqew73j8zhc0xhezx905fvytj5g4307czjf;
    - 35sBUp4t5t8gerEu9HswPiNhRSTnnS8qWX; and
    - 38WP9sta67jMzwPrzWfrGMci7qVCpX4cFY. *Id.* ¶ 16.
- 29.19 BTC was spent on blockchain transaction fees or dissipated, and the destination is still unknown. *Id.* ¶ 17.

In his Complaint, Plaintiff alleges that the Hacker is liable under the following causes of action: Computer Fraud and Abuse Act[1] ("CFAA") (Count I), New Jersey Computer-Related Offenses Act[2] (Count II), Fraud (Count III), Conversion (Count IV), Replevin under N.J.S.A. 2B:50-1 (Count V), and Unjust Enrichment (Count VI). Compl. ¶¶ 77-110. Plaintiff also seeks equitable relief against the Hacker and the Relief Defendants enjoining current and future holders of the stolen assets from transferring or disposing and disgorging such assets and seeks a constructive trust over the assets and an accounting of the assets (Count VII). *Id.* ¶¶ 111-119.

B. Procedural Background

On March 12, 2025, Plaintiff filed the Complaint, Motion for a TRO and a preliminary injunction, and a motion for expedited discovery, D.E. 6 ("Discovery Motion"). The same day the Court granted the Motion to the extent it sought a TRO, as well as the Discovery Motion. D.E. 4 ("Opinion"). Pursuant to Federal Rule of Civil Procedure 65(b)(3), the Court set an expedited briefing schedule and a hearing on the Motion for a preliminary injunction on March 20, 2025. D.E. 5. The Court also ordered that, by March 13, 2025, Plaintiff shall serve a copy of the TRO on the Relief Defendants and file a certification that he has done so. *Id.* Plaintiff timely filed an adequate certification on March 13, 2025. D.E. 7. No party filed opposition briefs and, other than Plaintiff, no party appeared at the Hearing on March 20, 2025.

II. LEGAL STANDARD

"Preliminary injunctions and TROs are extraordinary remedies that are not routinely granted." *Gentile v. Secs. and Exch. Comm'n*, No. 19-5155, 2019 WL 1091068, at *2 (D.N.J. Mar. 8, 2019) (citing *Kos Pharm., Inc. v. Andrx. Corp.*, 369 F.3d 700, 708 (3d Cir. 2004)). The decision

[1] 18 U.S.C. §1030 *et seq*.
[2] N.J.S.A. § 2A:38A.

to grant such relief is within the discretion of the district court. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006).

The primary purpose of preliminary injunctive relief is "maintenance of the status quo until a decision on the merits of a case is rendered." *Acierno v. New Castle Cnty.*, 40 F.3d 645, 647 (3d Cir. 1994). In order to obtain a TRO or a preliminary injunction, the moving party must show:

> (1) a reasonable probability of eventual success in the litigation, and (2) that it will be irreparably injured . . . if relief is not granted . . . . [In addition,] the district court, in considering whether to grant a preliminary injunction, should take into account, when they are relevant, (3) the possibility of harm to other interested persons from the grant or denial of the injunction, and (4) the public interest.

Reilly v. City of Harrisburg, 858 F.3d 173, 176 (3d Cir. 2017) (citing *Del. River Auth. v. Transamerican Trailer Transp., Inc.*, 501 F.2d 917, 919-20 (3d Cir. 1974)).

The movant bears the burden of establishing "the threshold for the first two 'most critical' factors . . . . If these gateway factors are met, a court then considers the remaining two factors and determines in its sound discretion if all four factors, taken together, balance in favor of granting the requested preliminary relief." *Id.* at 179. A court may issue an injunction to a plaintiff "only if the plaintiff produces evidence sufficient to convince the district court that all four factors favor preliminary relief." *AT&T v. Winback & Conserve Program, Inc.*, 42 F.3d 1421, 1427 (3d Cir. 1994) (internal marks and citations omitted); *see also P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 508 (3d Cir. 2005) ("The burden lies with the plaintiff to establish every element in its favor, or the grant of a preliminary injunction is inappropriate.").

III. ANALYSIS

The standard for a preliminary injunction and a TRO is the same. *See Reilly*, 858 F.3d at 176. Plaintiff relies on the same evidence for a preliminary injunction as he does for the TRO which the Court previously granted—namely Plaintiff's declaration, D.E. 2-2, which attested to

the relevant facts and attached documentary evidence, including a report prepared by Blockchain Forensic on the "theft and subsequent movements" of Plaintiff's Bitcoin, BF Report. Plaintiff's counsel represented at the Hearing that the facts have not changed since Plaintiff submitted his declaration and that he would testify to the same facts set forth in his declaration if testifying at the Hearing. No evidence to the contrary was submitted at the Hearing and no party opposed the Motion.[3] Therefore, the Court's analysis will largely mirror the analysis it conducted when granting the TRO. Opinion.

A. Likelihood of Success on the Merits

As a general rule, courts may not freeze a defendant's assets as part of a TRO or preliminary injunction in a case where only money damages are sought. *Grupo Mexicano de Desarrollo S.A. v. Alliance Bond Fund, Inc.*, 527 U.S. 308, 333 (1999). However, Plaintiff seeks the equitable remedy of a constructive trust over the stolen Bitcoin assets. "There is an exception to the general ban on prejudgment asset restraints where an equitable remedy is sought." *Nail All., LLC v. TTN Beauty*, No. 21-3140, 2021 WL 2646989, at *2 (D.N.J. Mar. 10, 2021). Therefore, as the TRO seeks such asset restraints, the Court will focus on Plaintiff's constructive trust claim, which provides for the availability of the equitable relief Plaintiff seeks.

The elements of a claim for constructive trust under New Jersey law are (1) a "wrongful act"; (2) "caused the property to come into the hands of the recipient"; and (3) "the recipient will be 'unjustly enriched' if it is not returned." *Thompson v. City of Atlantic City*, 901 A.3d 428, 438 (N.J. Super. Ct. App. Div. June 28, 2006).

Plaintiff has established a likelihood of success on the merits of his constructive trust claim. He has set forth evidence that the Hacker committed "wrongful act[s]"—principally gaining

[3] Notice of the Motion and Hearing was provided to the Relief Defendants. D.E. 7.

unauthorized access to Plaintiff's computer and transferring millions of dollars' worth of Plaintiff's Bitcoin out of Plaintiff's control into crypto wallets controlled by the Hacker. *See generally* Pl. Decl.; BF Report. Plaintiff has also put forward evidence that the Relief Defendants have come into possession or control of those assets—principally the BF Report showing the deposit addresses the funds were traced to that are associated with the Relief Defendant. BF Report at 11-21.[4]

Finally, Plaintiff has also set forth evidence that the Relief Defendants likely have been unjustly enriched from receipt of the assets in the form of fees charged for use of their services. *See* BF Report at 21 ("29.19 BTC was spent on blockchain transaction fees or dissipated . . . ."). Furthermore, the Court takes judicial notice of publicly accessible information on the fees that cryptocurrency wallet and exchange providers like the Relief Defendants charge based on use of their services, which likely account for at least some of the 29.19 BTC spent on transaction fees or dissipated as identified by the BF Report. *See, e.g.*, KRAKEN, *Fee Schedule*, https://www.kraken.com/features/fee-schedule (last visited March 20, 2025). Therefore, Plaintiff has established a likelihood of success on the merits of his constructive trust claim.

B. Irreparable Harm

In cases involving theft of cryptocurrency, many courts have recognized that the failure to promptly freeze the cryptocurrency leads to irreparable harm. *See, e.g.*, *Song v. Doe*, No. 24-809, 2024 WL 4632242, at *3 (M.D. Fla. Aug. 19, 2024) ("Plaintiff will suffer irreparable injury if the TRO is not granted because Defendants can quickly transfer the assets to another untraceable

[4] At the Hearing, Plaintiff advised the Court that a representative of FixedFloat represented that they do not hold cryptocurrency but were providing Plaintiff with information about the assets in question. However, FixedFloat did not appear at the Hearing and did not oppose the Motion seeking to enjoin it by freezing any assets in its possession, custody, or control. Therefore, there is no evidence in the record contradicting the BF Report documenting transfers of assets into addresses associated with FixedFloat.

cryptocurrency wallet or to offshore entities organized in unknown locations."); *Yogaratnam v. Dubois*, No. 24-393, 2024 WL 758387, at 4 (E.D. La. Feb. 23, 2024) ("Plaintiff has shown that irreparable harm will ensue absent a TRO, considering the speed with which cryptocurrency transactions are made, as well as the anonymous nature of those transactions."); *Heissenberg v. Doe*, No. 21-80716, 2021 WL 8154531, at *2 (S.D. Fl. Apr. 23, 2021) ("Because of the speed and potential anonymity of cryptocurrency transactions, the Plaintiff is likely to suffer immediate and irreparable injury if a temporary restraining order is not granted.").

The same is true here. Because of the anonymous nature of cryptocurrency transactions, Plaintiff may, unfortunately, never identify the Hacker. Freezing the Bitcoin Plaintiff has identified as rightfully belonging to him may be Plaintiff's only avenue for recovery. Under these circumstances, Plaintiff establishes that he will be irreparably harm if injunctive relief is not granted to freeze his Bitcoin pending the outcome of this litigation.

C. Harm to Others and the Public Interest

As set forth in Plaintiff's declaration, the assets at issue rightfully belong to Plaintiff and nobody else. According to Plaintiff's declaration and the BF Report, Plaintiff's Bitcoin was stolen from his cryptocurrency wallets and is in the process of being "distributed through a complex layering system designed to conceal the source of the money." BF Report ¶ 12. Therefore, it is not apparent that there is any significant harm to others or to the public interest that would result if the Motion is granted. Furthermore, the Court notes that despite being notified of the TRO and the Hearing, none of the Relief Defendants opposed the relief sought or attended the Hearing. This gives further support to the Court's finding that the level of harm to others or the public interest, if any, does not weigh against granting a preliminary injunction under the circumstances present here.

D. The Court Will Waive the Bond Requirement

Federal Rule of Civil Procedure 65(c) generally requires the posting of a security bond when issuing a preliminary injunction. However, the Court may waive this security requirement. *See LCN Enters., Inc. v. City of Asbury Park*, 197 F. Supp. 2d 141, 154 (D.N.J. 2002). The Court must "balance the hardship to the defendant if security is required against the hardship to the plaintiffs if it is waived." *Id.* (citing *Temple Univ. v. White*, 941 F.2d 201, 219 (3d Cir. 1991)). Additionally, "the likelihood of success on the merits . . . tips in favor of a minimal bond or no bond at all." *People of State of Cal. ex rel. Van De Kamp v. Tahoe Reg'l Plan. Agrency*, 766 F.2d 1319, 1326 (9th Cir. 1985) (cleaned up), *amended*, 775 F.2d 998 (9th Cir. 1985).

Here, Plaintiff has established a strong likelihood of success on the merits. That showing, coupled with the lack of harm on the enjoined parties (as evidenced by their lack of opposition and lack of attendance at the hearing), weigh in favor of waiving the bond requirement here. Therefore, the Court will waive the Fed. R. Civ. P. 65(c) bond requirement in this case.

IV. CONCLUSION

For the foregoing reasons, the Court will **GRANT** the Motion and will enter a preliminary injunction freezing Plaintiff's stolen Bitcoin pending the outcome of this case or until further order of the Court. An appropriate Order follows.

Dated: March 21, 2025

Evelyn Padin, U.S.D.J.